STORAGE, MANAGEMENT AND DISTRIBUTION OF CONSUMER INFORMATION

Related Applications

[0001] The present application claims the benefit of U.S. Provisional Patent Application Serial No. 60/223,232, filed August 4, 2000, hereby incorporated by reference as if set forth fully herein.

Technical Field

[0002] The field of the present invention relates generally to systems and methods for the storage, management, and delivery of user or consumer information on or over a network.

Background of the Invention

[0003] As information technology and network technology become more prolific, people find themselves repeatedly and manually inputting the same data into different computer systems. For example, consumers may find themselves having to manually input their personal and billing information via each vendor website through which they choose to complete an electronic commerce ("e-commerce") or mobile commerce ("m-commerce") transaction. As the number of secure websites grows, consumers also find themselves having to manage numerous usernames and passwords. Thus, there is a need for a convenient and secure system for automating the management of consumer information.

[0004] Automated or partially automated solutions for managing information historically have largely been localized processes. Using conventional techniques, users are able to create and store data files containing personal information on their

personal computers or other client devices, such as personal digital assistants ("PDAs"), pagers, mobile telephones, etc. The data elements in such data files can be shared using specialized applications for filtering data out of the data file and into another application. However, such systems typically require a permanent download of proprietary data management software that might not be compatible among different devices. In addition, the data management software and data files are often stored on only a single personal computer or computerized device. If the personal computer or other computerized device becomes lost or stolen, the user's data may no longer be accessible, and might end up in the possession of another person. If the personal computer or other computerized device crashes, the data can easily be lost.

[0005] Accordingly, there remains a need for a more secure, flexible and convenient system for storing information and a method for allowing the user to manage and distribute that information using a personal computer or other network-connected device. There further remains a need for such a system and method that provides central information storage and does not require a permanent download of proprietary software to a client device for management and distribution of the information.

Summary of the Invention

[0006] The present invention generally relates to systems and computer-implemented methods and associated computer-readable media for storing, managing and distributing consumer information. According to certain embodiments, an information account is stored in a central data repository accessible via a network. The information account may comprise a plurality of consumer information elements associated with a consumer. The consumer information elements are preferably, but need not be, stored in a tagged data format.

[0007] In accordance with one embodiment, a host server hosting a database management system for accessing the information account receives a request from a network device, responsive to an input command supplied by the consumer, for selected consumer information elements. In response to the request, the host server may filter the selected consumer information elements from the information account and transmit the filtered consumer information elements to the network device. The selected consumer information elements may be filtered from the information account using a style sheet or other suitable filtering mechanism.

[0008] In various embodiments, the request for selected consumer information elements may also include consumer authentication information. Prior to filtering the selected consumer information elements from the information account, the host server may authenticate the consumer based on the authentication information. The consumer may, in certain embodiments, be authenticated while accessing a first web page file and a single sign-on mechanism may be invoked so that the consumer will not be required to resubmit the consumer authentication information upon accessing a subsequent web page file prior to expiration of a time-out period.

[0009] According to one or more embodiments, the network device may comprise a client device executing a browser. The browser may access a web page file that includes an instruction that causes the browser to request a client-side application from the host server. Preferably, the client-side application temporarily resides on the client device and is configured to manage the request/response process for the network device. The client-side application may receive the filtered consumer information elements from the host server and integrates the filtered consumer information elements into a vendor's business process on behalf of the consumer. For example, the client-side application may auto-populate the filtered consumer information elements into at least one input field of the web page file and may allow the consumer to interact with the browser in order to submit the auto-populated web page file to the vendor server for processing. The consumer may edit the auto-populated consumer information elements or input additional consumer information elements. The client-side application may transmit the edited or added consumer information elements to the host server for storage in the information account.

[0010] In alternative embodiments, the network device may comprise a vendor server interacting with a client device. In such embodiments, the vendor server may execute a server-side application for interacting with the database management system of the host server. The server-side application may receive the filtered consumer information elements from the database management system and integrates the filtered consumer information elements into a vendor's business process on behalf of the consumer. For example, the server-side application may auto-populate the filtered consumer information elements into at least one input field of the web page file and may transmit the auto-populated web page file to the browser for display to the consumer. Any edits or additions to the consumer information elements that are made by the consumer may be passed to the server-side application and then

on to the host server for appropriate storage in the information account. Further attributes and advantages will become apparent from the following detailed description of certain exemplary embodiments, the appended drawings and the claims.

Brief Description of the Drawings

FIG. 1 is a high-level block diagram illustrating a system in accordance with one or more exemplary embodiments of the present invention as disclosed herein.

FIG. 2 is an abstract illustration of an information account in accordance with exemplary embodiments of the present invention as may be used, for example, in the system illustrated in FIG. 1.

FIG. 3 is an abstract illustration of another information account in accordance with other exemplary embodiments of the present invention as may be used, for example, in the system illustrated in FIG. 1.

FIG. 4 is an abstract illustration of an exemplary database schema in accordance with certain exemplary embodiments of the present invention.

FIG. 5 is a generalized interaction diagram illustrating the interaction between various system components of certain exemplary embodiments of the present invention.

FIG. 6 is a generalized interaction diagram illustrating the interaction between various system components when a new information account is created by a consumer via a vendor's website, in accordance with one or more exemplary embodiments of the present invention.

FIG. 7 is a generalized interaction diagram illustrating the interaction between various system components in an exemplary wireless environment.

Detailed Description of Exemplary Embodiments

[0011] In one or more embodiments, a system and method are provided for enabling consumers to store and maintain a comprehensive information profile (hereinafter "information account") in a centralized data repository that is accessible over a distributed electronic network, such as the Internet. The information account may be used to store any type of data desired by the consumer, including, for example, demographic information, financial information, medical information,

family information, contact information, documents, multimedia files, etc. The centralized data repository is preferably accessible via a network by any authorized network device. In various embodiments, no specialized application programs are required to be permanently downloaded to the consumer's network device in order to access the information account.

[0012] According to certain embodiments, at the consumer's direction, selected information in the information account may be accessed and, if desired, shared with authorized vendors, business partners or any other entity that requires certain of the consumer's information. The terms "vendor" and "business partner" are used herein in a general sense to refer to persons, businesses, enterprises or entities that make products or services available to consumers. As used herein, the terms "consumer," "buyer," and "user" are interchangeable.

[0013] Server-side software or temporary client-side software may, in some embodiments, be used to manage communications with the information account and to automatically integrate that consumer information into a process executed by a network device. As an example, the network device may execute a business process relating to a consumer-initiated activity, such as a retail transaction. The server-side software or temporary client-side software may receive consumer information from the information account and use that information to automatically populate the input fields of a form that is to be submitted to a vendor's server or other network device during an application, registration or transaction process.

[0014] The data in the information account is preferably stored using a tagged data format. In one embodiment, the data in the information account may be stored using the eXtensible Markup Language (XML) data format, which is an open standard for describing data from the World Wide Web Consortium ("W3C"). As is known in the art, XML tags are used to define the types of information that are represented by the data element. The XML standard provides a great deal of flexibility in that custom tags may be defined for any type of information that the consumer may desire to store in the information account. Using any well-known XML-related querying, parsing, transforming and/or filtering techniques, individual data elements in the information account may be accessed, updated, deleted, created, or otherwise manipulated.

[0015] The information account may be structured as one or more data aggregates, e.g., XML data aggregates. An entire XML data aggregate is stored

within a data field of a database table. This data field is a long text field containing all of the information associated with the given record. In one embodiment, all consumer information in the information account may be stored in a single XML data aggregate comprising consumer information elements and sub-elements. Attributes may also be associated with any element and sub-element in order to provide additional information. A transformation or filtering mechanism, such as "Style Sheets," may be applied to the single XML data stream in order to extract only selected data elements therefrom at the direction of the consumer.

[0016] In an alternative embodiment, the information account may be normalized into a plurality of discrete data aggregates, each aggregate representing a predetermined "information product." An information product refers to a package of consumer information relating to a specific product or service offered by a vendor. For example, a mortgage information product might contain all consumer information that would be required to complete a lender's mortgage application. Individual information products may be retrieved from the information account and transmitted to authorized vendors at the request of the consumer.

[0017] Access constraints implemented in a system of the present invention according to one or more embodiments as described herein allow for the establishment of "exchanges." An exchange refers to a group of entities that are authorized to accept consumer information from the information account at the request of the consumer. In other words, the information account may be used to retrieve information for use in commerce with any vendor that is a member of the exchange. In much the same way that a consumer may have several different credit cards or debit cards that are each accepted only by certain merchants, the consumer may have several information accounts that are each valid only on specified exchanges.

[0018] Exchanges may be accomplished through inflow and/or outflow constraints. An inflow constraint implemented by an exchange may, for example, dictate that only information accounts associated with specific other exchanges will be accepted or that no information accounts associated with other exchanges will be accepted. An outflow constraint may dictate that information accounts associated with an exchange may only be used within that exchange and within no other exchanges. Various business situations and partnerships may drive the implementation of inflow and outflow constraints. Revenue sharing models may be

established in order to provide financial incentives to exchanges and/or individual vendors that facilitate the creation of an information account or the use of an information account to complete a transaction.

[0019] Exemplary embodiments of the present invention will now be described with reference to the drawings, in which like numerals represent like elements throughout the several figures. A high-level block diagram of a system in accordance with an exemplary embodiment of the present invention is shown in and described with reference to FIG. 1. As shown, a central data repository **102** is provided for storing consumer information that may be easily accessed from any network device attached to the network **106**. The network **106** may comprise any telecommunication and/or data network, whether public or private, such as a local area network, a wide area network, an intranet, an internet and any combination thereof and may be wireline and/or wireless. Various methodologies as described herein may be practiced in the context of distributed computing environments. The network **106** thus provides for the open and seamless distribution of consumer information to and from the information account **110**.

[0020] In the system illustrated in FIG. 1, the exemplary operating environment encompasses various network devices for accessing and reading associated computer-readable media having stored thereon data and/or computer-executable instructions for implementing various methods of the present invention of data storage, management and distribution. Generally, a network device includes a communication device for transmitting and receiving data and/or computer-executable instructions over the network **106,** and a memory for storing data and/or computer-executable instructions. A network device may also include a processor for processing data and executing computer-executable instructions, as well as other internal and peripheral components that are well known in the art (e.g., input and output devices.) As used herein, the term "computer-readable medium" describes any form of computer memory or a propagated signal transmission medium. Propagated signals representing data and computer-executable instructions are transferred between network devices.

[0021] A network device may generally comprise any device that is capable of communicating with the resources of the network **106**. A network device may comprise, for example, a network server **108** & **114**, a client device **104**, a wireless client device **104a** or a dedicated storage device (e.g., the central data repository **102**.)

In the embodiment shown in FIG. 1, a host server **108** hosts the software for interacting with the central data repository **102** and for communicating with other network devices. The host server **108** may interact with the central data repository **102** via the network **106** or via a direct communication link **111**. A vendor server **114** hosts vendor web page files **116** comprising a vendor website, through which products or services may be offered to consumers.

[0022] A client device **104** may comprise a desktop computer, a laptop computer and the like. A wireless client device **104a** may comprise a personal digital assistant (PDA), a digital and/or cellular telephone or pager, a handheld computer, or any other mobile device. These and other types of client devices **104** & **104a** will be apparent to one of ordinary skill in the art. For convenience, the following explanation will be made with reference to a client device 104 generically, but, unless otherwise indicated, it will be understood that the principles and concepts described will also encompass wired or wireless devices, such as wireless client device **104a** illustrated in FIG. 1.. Moreover, although exemplary embodiments will be described herein in the context of the Internet or a web-based environment, it will be appreciated that the various principles and methods of operation will be applicable or may be practiced in other environments as well.

[0023] According to a preferred embodiment, a client device **104** may execute a browser **112** or another suitable application for interacting with web page files **116** hosted by a vendor server **114** and other network devices. Through the graphical user interface provided by a displayed web page file **116**, the vendor may require the consumer (i.e., the operator of the client device **104**) to input certain information pertaining to or associated with the consumer. The present invention allows the consumer to direct that the requested information be transmitted from the information account **110** to the client device **104** for processing. Although exemplary embodiments of the present invention will be described herein in the context of a web-based environment, those skilled in the art will appreciate that other environments are suitable as well.

[0024] The description of exemplary embodiments with reference to FIG. 1 assumes the existence of a previously created information account **110**. An example illustrating actual creation of an information account **110** will be described below with reference to FIG. 6. In general, the information account **110** may be any data structure for storing consumer information. Preferably, however, the information

account **110** is stored as a tagged data structure, such as one or more XML data aggregates. The data in the information account **110** is preferably encrypted so that anyone gaining unauthorized access to the information account **110** will not be able to read the data. Also, in a preferred embodiment, each information account **110** in the central data repository **102** is encrypted separately, so that someone authorized to access the information account of one consumer may not also gain access to the information account of another consumer.

[0025] In accordance with a preferred embodiment, the consumers may maintain sole responsibility for storing and updating the information in the information account **110**. Only the consumer, or those authorized by the consumer, may use the information account **110** to complete e-commerce or m-commerce activities. Consumers create an information account **110** either through a website hosted by the host server **108** or a website hosted by a vendor server **114**. For example, after manually completing a form displayed by a vendor's website, the consumer can choose to create an information account **110** and have the consumer information stored therein.

[0026] Upon creation of an information account **110**, a consumer may be given an identification number, a username and/or a password. Other types of consumer authentication information are known in the art and may also be used in the context of the present invention. The system of FIG. 1 provides the consumer with a variety of methods of accessing the information account **110**, transferring selected information to a vendor and/or allowing a vendor limited and constrained access to the information account **110**, as described in further detail herein.

[0027] In one embodiment of the present invention, a single sign-on mechanism may be provided to allow a consumer to "sign-on" (provide username and password, etc.) for authentication to access an information account **110** at only a first website. The authentication status may then "follow" the consumer as the consumer accesses subsequent websites. At such subsequent websites, a consumer who has activated the single sign-on mechanism will not be asked to re-authenticate himself. For example, the host server **108** may maintain an authentication table (not shown) that records the consumer authentication information, the sign-on time and a browser identifier. When the consumer accesses a subsequent website that requires sign-on for accessing the information account **110**, the client-side application **105** may communicate the browser identifier to the host server **108**. The host server **108** may

use the browser identifier to look up the consumer authentication information previous sign-on time in the authentication table. The previous sign-on time may be compared to the current time in order to determine whether a time-out interval has expired. If the time-out interval has not expired, the host server **108** may acknowledge that the consumer is authenticated.

[0028] A web page file **116** displayed by the browser **112** may include input fields for the input of consumer information. The web page file **116** may also include an instruction (e.g., a "call") that causes the browser **112** to download and execute a client-side application **105**. JAVA applets are well known client-side applications and are particularly suited for use in various embodiments due to their platform-independent nature. However, any other type of client-side application may be used without departing from the spirit and scope of the present invention. The client-side application **105** resides in temporary memory storage of the client device **104**, such as cache memory or the like, and may be removed from the client device **104** after its execution is complete. The client-side application **105** is specific to the browser session only and not to the client device **104**. Multiple client-side applications **105** may be executed at the same time if multiple browser windows are executed by the client device **104**. The client-side application **105** provides functionality for facilitating communications between the browser **112** executed by the client device **104** and the database management system ("DBMS") **109** of the host server **108**.

[0029] One responsibility of the client-side application **105** is to provide authentication information associated with the consumer and the vendor to the host server **108**. Depending on the desired level of security within the system, authentication information may comprise a username, user ID, password, key, certificate and the like. Authentication information regarding the vendor may be embedded within the web page file **116** for extraction by the client-side application **105**. Alternatively, the client-side application **105** may communicate with the vendor server **114** to retrieve such vendor authentication information. Authentication information regarding the consumer may be supplied by the consumer via a user interface displayed by the client-side application **105**. Communications relating to authentication information may be accomplished using a secure transmission protocol or handshake, such as the secure shell BSD, Point to Point Tunneling Protocol (PPTP), also commonly know as Virtual Private Network, and/or secure socket layering (SSL) protocol. Other methods for achieving a secure connection over the

network **106** will be apparent to those of ordinary skill in the art. Authentication information may also be encrypted and transmitted over an open network using any appropriate protocol.

[0030] The client-side application **105** is also responsible for determining the type of consumer information that is required by the input fields of the displayed web page file **116**. After determining the type of consumer information that is required, the client-side application **105** may formulate a database query in a language that is understood by the DBMS **109**. At a minimum, client-side application **105** communicates enough information to the DBMS **109** regarding the required consumer information so that the DBMS can formulate a database query. In one embodiment, the DBMS **109** exposes an application program interface ("API") that can be utilized by the client-side application **105**. An example of one such API is known as the Simple Object Access Protocol ("SOAP"). SOAP is a protocol that provides for interoperability between heterogeneous HTTP-based software and XML-based software. SOAP provides access to services, objects, and servers in a platform-independent manner. Since SOAP relies on HTTP as the transport mechanism, and most firewalls allow HTTP to pass through, SOAP endpoints may usually be invoked from either side of a firewall.

[0031] The client-side application **105** may transmit the database query (or information to form the database query) to the host server **108** along with the above-mentioned authentication information over a secure connection. In such a scenario, the authentication information and the query information may be passed to the DBMS **109**. The DBMS **109** attempts to authenticate the vendor and the consumer using the authentication information and corresponding information that was previously stored in the data repository **102**. If authentication is successful, the DBMS **109** queries the information account **110** using the appropriate database connectivity protocol, such as the Open Database Connectivity ("ODBC") protocol, the Java Database Connectivity Protocol ("JDBC"), or any other suitable protocol.

[0032] As mentioned above, the data in the information account **110** may be encrypted. Thus, in response to the query, the DBMS **109** may receive an encrypted search result. The search result, for example, may be in the form of a stream of XML data that has been filtered from the information account. The DBMS **109** or other program module executed by the host server **108** may be responsible for decrypting

the search result. The decrypted search results may then be transmitted to the client-side application **105** via the previously established or a new secure connection.

[0033] In the alternative, the client-side application **105** may manage authentication and querying as separate processes. As an example, authentication may be handled using a secure connection as described above. Upon acknowledgment of authentication, the secure connection may be closed and the query process may be handled using open network communication protocols. In response to the query, the encrypted search result may be transmitted to the client-side application **105** over the open network and the client-side application **105** may be responsible for decryption.

[0034] The client-side application **105** may also be responsible for parsing the data elements included in the search result and auto-populating the parsed data into the input fields of the displayed web page file **116**. Again, the client-side application **105** may translate the XML data into HTTP data using SOAP or another suitable protocol. Those skilled in the art will appreciate that in certain embodiments, especially where user verification of the consumer information is not required, the client-side application **105** may transmit the consumer information directly to the vendor server **114** without populating the consumer information into the displayed web page file **116**. If the input fields are auto-populated, the consumer has the opportunity to verify the information displayed in the input fields, make any necessary modifications, and then interact with the displayed web page file **116** to submit the information to the vendor server **114**. Any modifications to the consumer information that are made by the consumer may be detected by the client-side application **105**, which may then transmit the modified data back to the host server **108** for an appropriate update of the information account **110**. In addition, the client-side application **105** may determine whether the consumer inputs new data into the input fields, and if so, transmit that new information to the host server **108** for storage in the data repository **102**. The consumer may interact with the displayed web page file **116** to submit the consumer information to the vendor server **114**. The vendor server **114** may then process the consumer information, as needed, by way of a processing module.

[0035] In an alternative embodiment, a server-side application **107** may be employed instead of a client-side application **105** to manage communications with the host server **108**. An authorized server-side application **107** may receive consumer

information directly from the host server **108** and present that consumer information to the client device **104** (e.g., via the browser **112**) for display to the consumer. A web page file **116** hosted by the vendor server **114** may be accessed and displayed by the browser **112** of the client device **104**. The displayed web page file **116** may present a user interface for input of consumer authentication information. In a preferred embodiment, the consumer authentication information is transmitted from the client device **104** to the host server **108** for authentication of the consumer. In addition, the client device **104** may also transmit a request that a "ticket" be provided to the vendor server **114**.

[0036] As used herein, the term "ticket" refers to a temporary authorization for at least partial access to a consumer's information account **110**. Although not shown in the figure, an information account **110** may be associated with a data table or other data structure that correlates one or more tickets with a set of consumer-defined attributes. The consumer-defined attributes may determine such things as the number of times that the password may be used to access the information account **110** (e.g., one-time use), any period of validity associated with the ticket (e.g., ticket expires one week from issuance), whether the ticket carries read, write and/or modify privileges, etc. The ticket attributes may also include any number of identifiers, such as a vendor identifier, a data identifier, and filter identifiers, which may be used to ensure that the party using the ticket is in fact authorized to do so, and to ensure that only authorized data is filtered for release to that party.

[0037] Upon authenticating the consumer, for example by using standard browser authentication techniques, the host server **108** may redirect the browser **112** of the client device **104** to another web page data file **116** (e.g., another web page data file **116** hosted by of the vendor server **114**), including the ticket as a parameter in the URL. In response to detecting the ticket, the vendor server may extract the ticket and pass it to the server-side application **107**. The server-side application **107** may then use the ticket to authenticate itself to the host server **108**, for example using SOAP or another suitable protocol.

[0038] In accordance with one embodiment of the present invention as described herein, a ticket generated by the host server **108** may be a "Globally Unique Identifier" ("GUID"). A GUID is a unique number that is computed by adding the time and date to a network adapter's internal serial number. Other unique identifiers may also be used as tickets in accordance with the present invention. The ticket may

be encrypted. For example, the ticket may be encrypted using the vendor's public key and the resulting binary encrypted blob may be base64 encoded such that so that it can be included as a parameter in a URL. At the vendor server **114**, the parameter would need to be extracted from the URL, base64 decoded and then decrypted using the vendor's private key. These and other encryption methods will be apparent to one of ordinary skill in the art.

[0039] In an alternative embodiment, consumer authentication information may be submitted from the client device **104** to the server-side application **107** at the vendor server **114**. The server-side application **107** may then transmit the consumer authentication information and vendor authentication information to the host server **108** for authentication of both the consumer and the vendor. The consumer authentication information may be encrypted at the client device **104** and decrypted only at the host server **108**. Such an embodiment, however, places a significant amount of control over the consumer's data in the hands of the vendor, and thus may not be preferable.

[0040] The server-side application may be identified by an application identifier ("APPID"). The APPID may be associated at the host server **108** (e.g., by the DBMS **109**) with a particular filtering mechanism. As mentioned, style sheets are well-known and highly suitable filtering tools for use in conjunction with XML data. In response to authenticating the server-side application **107** and identifying the appropriate filter, consumer information may be filtered from the information account **110** and transmitted back to the server-side application **107**. The server-side application **107** may then parse the consumer information, for example, in order to auto-populate a form, which may or may not have been previously displayed to the consumer.

[0041] As in the case of the client-side application **105**, the server-side application **107** may receive decrypted consumer information from the host server **108** via a secure connection, or may receive encrypted consumer information via the open network. Thus, the server-side application **107** may be configured to perform decryption as necessary. The consumer information thus received from the host server **108** may be presented to the consumer for verification. Any modifications or additions made to the consumer information may be submitted back to the server-side application **107** for communication to the host server **108**. The DBMS **109** may then update and/or create the information account **110** in the appropriate manner. The

consumer may interact with the displayed web page file **116** to submit the consumer information to the vendor server **114**. The vendor server **114** may then process the consumer information, as needed, by way of a processing module.

[0042] Those skilled in the art will appreciate that the illustration and discussion of exemplary embodiments with reference to FIG. 1 is provided as a generalized example only. Specific details regarding data formats and network communication protocols have been omitted, as such details are well known in the art. Furthermore, the present invention is not intended to be limited to the use of any particular data formats or protocols. Any existing or future formats or protocols may be used without departing from the spirit and scope of the invention. Furthermore, many network components were not shown or discussed with reference to FIG. 1, such as gateways, routers, hubs, switches, firewalls, DNS servers, authentication servers, certificate authorities, and the like. The functions and roles of such network components are also well known in the art and need not be described in detail herein.

[0043] FIG. 2 provides an abstract illustration of an information account **110** in accordance with an exemplary embodiment of the present invention as described herein. In the illustrated embodiment, the consumer information is stored in the information account **110** as a single tagged (delimited) data stream. Those skilled in the art will recognize that XML provides a suitable tagged data format for use in connection with the present invention. However, other tagged data formats can be employed as well. Thus, references to the XML standard in connection with exemplary embodiments of the present invention are not intended to limit the scope of the present invention. The single XML data stream comprises a plurality of consumer information elements **202**, each having a unique tag **204** or identifier. A consumer information element **202** may be divided into any number and/or level of sub-elements **206**. As is well known in the art, an XML consumer information element **202** may also be associated with one or more attributes **208**. An attribute **208** may provide additional information about the content, structure or formatting of a consumer information element **202**.

[0044] A consumer information element **202** may comprise any type of data or information, including text strings, objects, files, applications, etc. Obviously, the more consumer information that is stored in the information account **110**, the larger the XML data stream will be. The size of the XML data stream is limited only by the

hardware and software limitations of the system (e.g., memory size, processor speed, bandwith, etc).

[0045] An information account **110** is preferably unique to a single customer. Each information account **110** stored in the data repository **102** may thus comprise a discrete XML data stream. Each information account **110** stored in the data repository **102** may be individually encrypted. For example, one method for encrypting an information account **110** may involve use of the consumer's public key. Accordingly, only someone having access to the consumer's private key will be able to decrypt the consumer's information. Many other and/or additional methods for encrypting information accounts **110** and/or the entire data repository **102** will occur to those skilled in the art.

[0046] Although not shown in FIG. 2, those skilled in the art will appreciate that a consumer information element **202** in one information account **110** may comprise a pointer or a reference to another data element or to another information account **110**. In one embodiment, a consumer may create, for example, a list of business contacts. A new information account may be created for each individual specified as a business contact by the consumer. Authentication data within the new information account may be set as "anonymous" so that the first consumer may retain access privileges. At some point later, however, the individual named as the business contact may be given control of the new information account by changing the associated authentication information to be unique to that individual. The first consumer may then be granted limited access privileges to continue to access the new information account of the business contact (e.g., by way of a ticket). Alternatively, the first consumer may retain a copy of the business contact information in his own information account.

[0047] FIG. 3 provides an abstract illustration of an information account **110** in accordance with other exemplary embodiments of the present invention. In the embodiment shown, an information account **110** is structured as multiple discrete XML aggregates **302a-c**. The discrete XML aggregates **302a-c** may comprise one primary "profile" record **302a** and one or more information product records **302b-c**. The profile record **302a** may include a general profile of information elements **304** associated with the consumer. Information product records **302b-c** contain consumer information elements that are specific to a particular product or service offered by a vendor. Aggregation of data elements according to information products allows quick

and efficient retrieval of specific consumer information from the information account **110** through a request-response system.

[0048] The number of aggregates or records included within the information account **110** of a given consumer depends upon the number of information products for which the consumer has elected to store information. For example, a consumer who has elected to store information about two separate products, such as a car loan and a mortgage loan, would have at least three data aggregates in his information account **110**. One such data aggregate would represent the primary profile record and each of the two other data aggregates would include information about one of the information products. Data aggregates may include but are not limited to the following information products: Home Loan, Auto Loan, Student Loan, Home Insurance, Auto Insurance, Life Insurance, Online Banking, Credit Card, Government Services, Education, Career, Travel, Retail, and Relocation. If a consumer creates or updates an information account via a vendor's web site and thereby inputs information regarding a new product, a new product record **302b-c** will be created in the information account. Each product record **302b-c** created for the consumer is of course associated with the primary profile record **302a**.

[0049] If an information account **110** is segmented into multiple discrete data aggregates, there may be a need for maintaining consistency among redundant data elements stored in multiple information products. "Latent referential processing" is one method for maintaining data consistency that is contemplated by the present invention. Latent referential processing in this context refers to the use of a series of pointers or references to flag data that is redundant across multiple products. According to latent referential processing, when a record **302a-c** is created or updated, redundant information elements that are stored in other data aggregates typically are not also updated until the next time the information account is accessed. For example, if salary information is updated in a home loan information product record, redundant salary information in the consumer's auto loan information product record will generally not be immediately updated. Thus, latent referential processing allows data inconsistencies to exist within the information account after an update.

[0050] As is shown and described with reference to FIG. 4, a transaction log may be maintained in the information account to record the date and time of the most recent update for each data record **302a-c**. Each time a request is made to access the information account, the DBMS **109** may first examine the transaction log to

determine which data element in a set of redundant data elements has most recently been updated. After determining the most recently updated data element, all other redundant data elements are updated to be consistent with the most recently updated data element. Upon completion of the latent referential processing, the request to access the information account may be granted. Accordingly, latent referential processing is a new way of storing and tracking information that addresses the need of providing quick access to information that will be accessed more frequently than it will be updated.

[0051] In another embodiment, redundancy and consistency concerns are addressed by normalizing the data aggregates of the information account **110** to the extent possible. For example, an information account **110** may be configured such that the consumer's profile record **302a** stores the majority of the consumer's personal information. The profile record **302a** may comprise predefined data elements, such as "first name," "middle name," "last name," date of birth," etc. The profile aggregate **302a** may also be expanded to include any additional and/or custom fields. Additional aggregates corresponding to information products **302c** may contain pointers **306** to the data fields within the profile aggregate **302a**. Thus, the information account **110** may be configured to store within one aggregate a single instance of an information element that is referenced by other aggregates. As information product aggregates **302c** are formed independently of the profile aggregate **302a**, data elements that are not unique to those information product aggregates **302c** may be ported into the profile aggregate **302a** if desired.

[0052] FIG. 4 illustrates an exemplary database schema **400** in accordance with one or more exemplary embodiments of the present invention as disclosed herein. In particular, the database schema **400** represents the situation where the information account **110** is segmented into multiple discrete data aggregates, as shown in FIG. 3. The database schema **400** may include a consumer authentication record **402** that stores consumer authentication information **404** such as, for example, a user ID, username, password, email address, access attempts, last attempt date/time, challenge word or phrase, challenge response, ticket parameters, and vendor credited with origination of the information account. These and other types of authentication information may be used to authenticate a consumer. The database schema **400** may also include a profile record **302a** that stores a primary information profile **304** of the consumer. There will typically be a one to one relationship between the consumer

authentication table **402** and the profile record **302a**. The exemplary database schema **400** also includes one or more information product records **302b-c** that store product-specific information. Each profile record **302a** may be associated with one or many information product records **302b-c**.

[0053] The profile record **302a** and each information product record **302b-c** may further be associated with a transaction log record **406**. Each time the profile record **302a** or an information product record **302b-c** is acted upon, detailed transaction information **408** may be recorded in a new transaction log record **406**. As mentioned above, transaction information **408** may be used for the purpose of maintaining consistency among redundant data elements. Another or additional purpose of the transaction information **408** is to provide the basis for all transaction billing and revenue sharing events. By way of example only, the transaction record **406** may identify the vendor server through which the information account **110** was created. The transaction record **406** may also identify the vendor server through which a transaction was completed using the information account **110**. A portion of any monies billed upon completion of a transaction may be shared with each of the vendor servers identified in the transaction record **406**.

[0054] FIG. 5. is a generalized interaction diagram illustrating the interaction between various system components of certain exemplary embodiments of the present invention in connection with consumer-controlled storing, managing and/or distributing information. The exemplary embodiments discussed with reference to FIG. 5 employ a client-side application **105**, such as an applet, to manage communication between the client device **104** and the host server **108**. Alternative embodiments employing a server-side application **107** instead of the client-side application **105** have been discussed above. Those skilled in the art will appreciate the differences between the interactions involving a client-side application **105** and a server-side application **107**.

[0055] The generalized interaction diagram begins at step **501**, where the consumer operates a browser **112** to retrieve a web page file **116** from the vendor server **114** via the network **106**, using a consumer browser. The web page file **116** retrieved from the vendor server **114** may be enabled for interaction with the consumer's information account **110** and may thus include an instruction that causes the browser **112** to download a client-side application from the host server **108**. At step **502**, the client-side application is downloaded from the host server **108** to the

browser **112**. At step **504**, the consumer interacts with the browser **112** to request use of the information account **110**, which in this example has already been created. The web page file **116** may display a selectable icon or other indicia that allows the consumer to request use of the information account **110**. Alternatively, the client-side application **105** may provide the interface for requesting use of the information account **110**.

[0056] Next at step **506**, the client-side application **105** displays a login interface to the consumer. The login interface may be displayed, for example, in the open display window of the browser **112**, in a pop-up window, or in any other suitable manner. At step **508** the consumer inputs consumer authentication information, which is transferred from the browser to the client-side application **105**. Consumer authentication information may comprise, for example, a username, user ID, password, challenge phrase, email address, etc. At step **510**, the user authentication information is combined with vendor authentication information and is sent to the DBMS **109**. Vendor authentication information may comprise a vendor ID, password, product IP, application ID, and the like. Vendor authentication information may be used to authenticate the vendor and to determine the manner in which consumer information is to be filtered from the information account **110**.

[0057] After the DBMS **109** receives the authentication information, it submits an authentication request to the data repository **102** at step **512**. The authentication request may be a database query to determine if the supplied consumer authentication information and vendor authentication information are consistent with previously stored authentication information. In response to authenticating the consumer and the vendor, the DBMS **109** performs one or more database queries at step **514** to retrieve consumer information elements from the information account **110**. Depending on the structure of the information account, the DBMS **109** may retrieve certain products (identified by product ID) from the information account **110**, or may retrieve a set of data elements filtered according to a vendor ID or an application ID. If consumer information is retrieved according to products, an iterative lightweight transfer ("LWT") process may be performed in order to get the best set of data elements for each new product ID. Lightweight transfer techniques are well-known in the art and generally involve the use of thin protocols and/or smart proxies that can cache results and perform buffered reads and writes, minimizing the number of network calls.

[0058] Once the DBMS **109** has retrieved the relevant consumer information, the consumer information elements may be merged (if appropriate) decrypted (if appropriate) and/or further filtered (if appropriate) at step **518**. Then, at step **520**, the resulting information elements are transmitted to the client-side application **105**, for example in the form of an XML data stream. At step **522**, the client-side application **105** parses the received XML data and transforms it into the required format for populating the input fields of the displayed web page file **116**. The client-side application **105** then auto-populates the input fields of the displayed web-page file **116** at step **524**. The consumer may interact with the browser **112** to edit or modify the auto-populated information at step **526**. Because there may be multiple web page files **116** associated with the vendor website, steps **524** and **526** are repeated until all data has been auto-populated and/or edited on every included web page. The client-side application **105** monitors the edit process to determine if the consumer desires to modify and/or supplement any of the consumer information elements.

[0059] The consumer may then interact with the browser **112** at step **528** in order to submit the consumer information that has been entered into the displayed web page file(s) **116** to the vendor server **114**. The vendor server **114** receives and processes the consumer information elements at step **530**. After processing the consumer information, the vendor server **114** preferably transmits a "success page" or other acknowledgement to the consumer's browser **112** at step **532**.

[0060] Either through a selectable icon or other indicia displayed on the success page or displayed by the client-side application **105**, or any other interactive means, the consumer may interact with the browser **112** at step **534** to submit an update request to the DBMS **109**. Update is an event whereby the information account **110** is updated to reflect any edits that the consumer may have made to the consumer information at step **526**. Thus, the present invention allows the consumer to update the information account **110** via a vendor's website. As another option, the consumer may elect to update the information account **110** at a later time directly via the host server **108**.

[0061] At step **536** the client-side application submits the consumer's XML data (possibly only the edited data) and the update request to the DBMS **109**. Then at step **538** the update request is submitted to the data repository for authentication. In the authentication process, consumer authentication information, vendor authentication information and, if appropriate, product identification information

(which are all included in the update request) are verified. Upon authentication of the update request, the XML data is validated at step **540** and the update is performed at step **542**. The DBMS then sends the update result (success or failure) to the client-side application **105** at step **544**, which in turn displays the update result to the browser **112** at step **546**. The exemplary generalized interaction diagram then ends at step **548**.

[0062] FIG. 6 is a generalized interaction diagram illustrating the interaction between main system components when a new information account is created by a consumer via a vendor's website. As mentioned, the consumer may create an information account by visiting a vendor's website that has been configured to interact with the system of the present invention according to the techniques described herein. The vendor's website may, for example, require the user to manually input consumer information into the input fields of a form. The user may then direct that an information account be created to store the consumer information, so that the consumer will not be required to manually enter the consumer information again on any participating website.

[0063] The exemplary embodiments discussed with reference to FIG. 6 employ a client-side application **105**, such as an applet, to manage communication between the client device **104** and the host server **108**. Alternative embodiments employing a server-side application **107** instead of the client-side application **105** have been discussed above. Those skilled in the art will appreciate the differences between the interactions involving a client-side application **105** and a server-side application **107**.

[0064] The exemplary interaction diagram of FIG. 6 begins at step **601**, where the consumer operates a browser **112** to retrieve a web page file **116** from the vendor server **114** via the network **106**, using a consumer browser. The web page file **116** retrieved from the vendor server **114** may be enabled for interaction with the consumer's information account **110** and may thus include an instruction that causes the browser **112** to download a client-side application from the host server **108**. At step **602**, the client-side application is downloaded from the host server **108** to the browser **112**. At step **604**, the consumer interacts with the browser **112** to input consumer information into the input fields of the vendor's website. The client-side application **105** monitors the input of consumer information at step **606**.

[0065] Next at step **608** the consumer interacts with the browser **112** in order to submit the consumer information to the vendor server **114**. The vendor server **114** receives and processes the consumer information elements at step **610**. After processing the consumer information, the vendor server **114** transmits a "success page" or other acknowledgement to the consumer's browser **112** at step **612**. Either through a selectable icon or other indicia displayed on the success page or displayed by the client-side application **105**, the consumer may interact with the browser **112** at step **614** to submit a request for creation of an information account **110** to the DBMS **109**. Thus, the present invention allows the consumer to create an information account **110** via a vendor's website. As another option, the consumer may elect to create an information account **110** at a later time directly via the host server **108**.

[0066] At step **616** the client-side application submits the consumer's XML data and the create request to the host server **108**. Then at step **618** the host server **108** transmits an information account creation interface to the browser **112**. The consumer inputs consumer authentication information via the information account creation interface at step **622** and the browser **112** passes the create request (which may include the consumer authentication information, the vendor authentication information, etc.) to the client-side application **105** at step **624**.

[0067] At step **626**, the create request is combined with the consumer's XML data and is sent to the DBMS **109**. In response to receiving the authentication information, the DBMS **109** submits an authentication request to the data repository **102** at step **628**. The authentication request may be a database query to determine if the supplied consumer authentication information and vendor authentication information are consistent with previously stored authentication information. In response to authenticating the consumer and the vendor, the DBMS **109** validates the consumer's XML data at step **630** and creates a new information account **110** at step **632**.

[0068] Once the information account has been created, the DBMS **109** sends the create result (success or failure) to the client-side application **105** at step **634**, which in turn displays the create result to the browser **112** at step **636**. At step **638**, the host server **108** creates an acknowledgment email to be sent to the consumer's email account. At step **640**, the host server requests and receives the consumer's email address from the DBMS **109**. At step **642** the consumer's acknowledgment

email is delivered to the consumer. The exemplary generalized interaction diagram then ends at step **644**.

[0069] FIG. 7. is a generalized interaction diagram illustrating the interaction between various system components in an exemplary wireless environment suitable for implementation of the present invention in connection with consumer-controlled storage, management and/or distribution of information. An exemplary wireless environment is suited for wireless devices such as digital or cellular telephones, personal digital assistants (PDAs), portable computers, and the like. Such wireless devices generally include a display device and an input device (keypad, touch screen, microphone, etc.), each of limited size and utility. The difficulty of inputting detailed information and commands into a wireless device makes it desirable to provide a system whereby the backend DBMS **109** is able to communicate directly with various remote web servers, thus eliminating a significant amount of user-interaction with the wireless device.

[0070] The generalized interaction diagram of FIG. 7 begins at step **701**, where the consumer operates a wireless client device **104a** to access the host server **108**. Accessing the host server **108** may involve, for example, calling a dedicated access number using a mobile telephone device or two-way pager. At step **702**, the wireless client device **104a** accesses the host server **108** via a wireless application ("WAP") gateway. At step **704**, the host server **108** returns a login interface to the wireless client device **104a**. At step **706** the consumer inputs consumer authentication information using an input device of the wireless client device **104a**. Consumer authentication information may comprise, for example, a username, user ID, password, challenge phrase, email address, etc.

[0071] At step **708**, the user authentication information is combined with vendor authentication and is sent to the DBMS **109**. Vendor authentication information may comprise a vendor ID, password, product IP, application ID, and the like. Vendor authentication information may be used to authenticate the vendor and to determine the manner in which consumer information is to be filtered from the information account **110**. After the DBMS **109** receives the authentication information, it submits an authentication request to the data repository **102** at step **710**. In response to authenticating the consumer and the vendor, the DBMS **109** performs one or more database queries to retrieve consumer information elements from the information account **110**. Depending on the structure of the information